Assumption Busters Workshop - Cloud Computing

Background: In 2011, the U.S. Federal Cyber Research Community conducted a series of four workshops designed to examine key assumptions that underlie current security architectures in cyberspace. These "Assumption Busters" meetings were designed to create an environment for developing novel solutions based on fundamentally different understandings of cyber problems and create a stronger basis for moving forward on well-founded assumptions.

The four topics discussed at the 2011 "Assumption Busters" Workshops included: defense-in-depth, trust anchors, malicious behaviors, and cloud computing. Participants of these workshops assessed the problems for each assumption as well as weaknesses that transcend these four categories.

Introduction: The fourth "Assumption Busters" workshop was held on 21 October 2011 at NIST in the Administration Bldg, Lecture Room D, in Gaithersburg, MD. The workshop focused on the assertion that "current implementations of cloud computing indicate a new approach to security." Over 40 participants from academic, government, industry and the research communities attended.

The meeting was divided into four sessions: Virtualization, Cryptologic Mechanisms, Risk-Based Distributed Data Processing, and Cloud Auditing Systems. Eleven attendees were given the opportunity to present highlights from submitted workshop papers related to these topics. Each presentation of current research activities was followed by discussion amongst participants about the central research concepts. These discussions included the fundamental assumptions about these concepts and the potential future research concepts of interest.

Researchers developing cyber security solutions were invited, along with researchers working on how to exploit or counter these solutions. The result was a robust debate of topics long held to be true in order to determine the extent that claims about cloud security are warranted. The adversarial nature of these debates assured that the threat environment was adequately reflected in the discussions and the research concepts that resulted from this workshop will have a greater chance of having a sustained positive impact on our cyber security posture.

This paper provides a brief summary of the information discussed at the workshop. It includes summaries of the presentations; identified benefits and challenges presented by cloud computing; and potential future research areas.

Workshop Assumption: **“**Current implementations of cloud computing indicate a new approach to security.”

Bottom Line: Participants of the workshop agreed with the assumption that current implementations of cloud computing indicate the need for a new approach to security. Participants proceeded by identifying the specific factors associated with cloud computing that indicate this new approach. While some factors introduced by the cloud present security benefits, participant also identified several security challenges that warrant further research.

Security Benefits Presented by Cloud Computing:

-- The group identified that the aggregation of security and network data supported by cloud computing may yield a more supportive environment for predictive analytics, including those related to cloud security. The volume and variety of data located on the cloud will increase the scope of analysis and potentially yield more accurate predictions. The group expressed the need for rapid cyber security methods similar to weather forecast and planning activity. For instance, one participant mentioned that the cloud may improve detection of malicious global activity patterns such as botnet swarming; thereby enabling a more timely and effective response.

-- Participants identified data distribution as a significant enhancement to security offered by the cloud. This opinion was formed on the basis that dispersing data throughout different areas of the cloud will inhibit attackers from easily extracting complete sets of data. However, participants also determined that data distribution will consequently lead attackers to counteract this impediment by attacking the sources of data. Contrary to attacks focused on individual data sets, attacks focused on the mechanisms/algorithms responsible for data distribution and data reassembly will have a more widespread impact. One participant also argued that although distributed data schemes may provide more security against non-sophisticated attackers, they will not serve as an impediment to sophisticated attackers.

Security Challenges presented by the Cloud:

-- In addition to existing attack amplifiers, participants identified that cloud computing will also introduce new attack amplifiers. However, the group also recognized that the homogeneity and connectivity of cloud computing may make early detection of these attack amplifiers more feasible. While some perceive homogeneity as a benefit of the cloud, one participant raised the point that homogeneity will magnify the impact of inevitable security failures. In particular, the impact of malicious insiders within provider and customer organizations becomes dramatically amplified by homogeneity.

-- Participants identified the benefits and challenges of implementing hardware in processors to support virtualization. Although virtualization was originally achieved solely using complex software techniques, it now benefits from added hardware support in processors. Despite improving process isolation, hardware solutions can be problematic when security flaws are discovered after widespread adoption of the hardware. Participants offered the example that a security flaw in a piece of hardware may involve an extensive recall while software security flaws will simply require the dispersion of a patch or upgrade. However, as one participant mentioned, many current compromised computers result from individual users failing to apply patches and updates. The participant continued by explaining that the number of computers that are compromised due to lack of patching and updating would ultimately be reduced by the cloud.

-- Relying on hypervisors could potentially yield adverse results. While hypervisors provide significant advantages by hosting multiple operating systems simultaneously, they also create a single point of failure where a particular vulnerability can be exploited across the entire infrastructure. The uniform attack surface available to attackers will impede efforts by providers to quarantine attacks. There is also concern over attacks resulting from the creation of new attack surfaces, such as side channel attacks.

-- Another challenge identified by workshop participants concerned implementation of Service Level Agreements (SLAs). While the group accepted agreement regarding the necessity of implementing SLAs with the cloud, opinions varied concerning which party should assume responsibility for security. Many argued that SLAs create too much of a liability to cloud providers and that the role of securing or encrypting data should be the responsibility of the consumer. Participants pointed out that forcing cloud providers to assume responsibility for security would inevitably drive up costs; thereby defeating the purpose of the cloud as an inexpensive solution. One participant discussed research concerning whether it would be possible to develop SLAs that allow cloud providers to appropriately allocate services based on the trust requirements stipulated in a user's SLA. Participants went on to discuss the development of an SLA specification language that enables cloud providers to effectively manage multiple user workloads. Researchers are currently using the prototype, MorphoSys, to verify the viability of the SLA specification language. One participant also discussed the opportunity for Colocation as a Service. Colocation as a Service enhances trust by presenting the opportunity for cloud users to control colocation decisions such as forming compatible coalitions of workloads. However, one participant also argued that offering multiple levels of service options to users will render ineffective if users are unable to understand the options available.

-- It was also determined that cloud security must involve auditing systems capable of factoring in the clients, servers, and networks that the communications traverse. Auditing challenges were identified as a byproduct of cloud computing because of the enhanced movement and dispersion of data. There was speculation during the discussion as to whether or not auditing systems exists that are capable of tracking moving targets.

-- One participant made the argument that the cloud was not so much a problem as were the personal devices connected to the cloud. Users who allow large numbers of applications to run on their devices significantly enhance their risk of an attack. In order to protect the cloud as a whole, providers must protect the weakest links in the system.

-- One participant discussed the challenges in securing the cloud against botnets, or "Dark Cloud." The recommended solution is referred to as the "White Cloud" and involves the coordinating routers across networks in order to mitigate botnet effectiveness by installing filters at selected, strategic routers.

Areas for Future Research and Exploration

Hardware vs. Software Support to Virtualization – Participants recognized the need for research concerning the security advantages and disadvantages of implementing hardware solutions to support virtualization.

Need for Case Studies – Participants recognized that attack avoidance will yield a greater return on investment than detection and recovery. Thus, there is a need for case studies that describe situations where security has been successfully addressed and implemented. The case studies should present a diversity of situations involving particular configurations and threats, as well as comment on the business use case for additional security.

Research in Detection and Game Theory – The complex and diverse environment of the cloud reveals the need for future research concerning the application of detection and game theory to cloud computing. Research should address the attacker's alternative way of thinking compared to our own and how to handle elements of security in an already compromised environment. Participants offered the example of methods for securing keys in already compromised environments.

Research in Centralized Security Management Strategies – The new environment introduced by the cloud will require further research into how centralized security management strategies can be applied to cloud computing. To improve the overall security of centrally stored data, the group recognized the need for formal methods and crypto techniques that are resultant of enhanced research environments and better data. Recommended solutions for securely distributing centrally stored data included implementations of a crypto approach that may potentially yield opportunities to apply different crypto algorithms for different classes of data. Participants agreed that overall improvements to crypto management are necessary to ensure that data is distributed and reassembled securely. However, one participant emphasized the need for a holistic approach to system development and cautioned against overreliance on cryptography.

More Rigorous Definitions – There was significant concern regarding the lack of concrete definitions in cyber security and the role(s)/ activities of malicious actors. For example, participants identified the need for rigorous definitions concerning sophisticated and unsophisticated attackers, and the behaviors they exhibit. The development of more rigorous terminology would improve the overall understanding of the nature of attacks and prevent inappropriate use/application of terminology.

Service Level Agreements - Regarding SLAs, there is a serious need to rigorously define the levels of service offered, and the attendant security responsibilities, of Service Level Agreements associated with cloud computing. One participant mentioned their research in developing an SLA specification language. However, there is also the need for continued research pertaining to the development of compositional security SLAs. One participant offered the recommendation that third parties be used as a mechanism for assessing performance and ensuring trust. A participant also identified the need to ensure that third party services remain transparent to users. Among recommendations for developing cloud SLAs, one participant outlined the need to: (1) *define and verify* the trustworthiness of cloud computing components across dimensions related to both performance and security, (2) *design mechanisms* that deliver desirable levels of trustworthiness along each of these dimensions as well as enable tradeoffs across these dimensions, and (3) *expose these tradeoffs* to cloud customers and system integrators in practical and usable ways.

Sufficient Auditing Mechanisms – The group identified a substantial need for the exploration of auditing mechanisms capable of tracking moving data. In addition to providing availability and performance measurements, these auditing mechanisms should possess the capacity to quantify, measure, and verify security in the cloud. Subsequently, analysis of the metrics produced by sufficient auditing mechanisms will enhance the overall understanding of the cloud environment. One participant recommended developing secure IP geolocation algorithms to detect targets in the presence of untrustworthy measurements and developing secure measurement protocols to discount target measurements deemed untrustworthy.